Storage Procedures

Pick-up / Delivery Schedule

Storage vendors will pick-up and deliver your cartons. All requested orders that are sent to the storage vendor by 4:00 p.m. will be delivered or picked-up on the next work day. Normal hours of operation are Monday through Friday 8:00 a.m. to 5:00 p.m. locally (except holidays). If a storage vendor cannot fulfill a request because you or your alternate contact are not available, your department will be charged for all fees. NO RUSH OR EMERGENCY RETRIEVALS WILL BE ACCEPTED WITHOUT PRIOR APPROVAL FROM RIM. If you have an emergency situation, please contact Phil Hasselvander at Vnet 806-3398 (703-886-3398) or Chris Moses at Vnet 806-7117 (703-886-7117).

New Storage

Obtain off-site storage supplies (approved record storage cartons and barcode labels) from your storage vendor through the supply request form on RIM's website.

The MCI Box Inventory Form can also be obtained on RIM's website.

Follow these steps to send cartons to storage:

1. Complete the Inventory Form (see instructions below).
2. Two identical peel-off, die cut, barcode labels are provided. Affix the small barcode label to the Inventory Form where indicated. This barcode number is your carton number. This is the carton number you will use to retrieve and refile your cartons.
3. Affix the larger barcode label to the narrow side of the carton under the hold handle.
4. The inventory form is not a two-part form. After affixing the barcode label, make a copy of this form for your files.
5. Schedule a pick-up by completing the new storage pick-up request form on the RIM website. If you are not sure which city you should choose, please contact Phil Hasselvander at Vnet 806-3398 (703-886-3398) or Chris Moses at Vnet 806-7117 (703-886-7117).
6. You must EMAIL your inventory form to RIM at rim@mci.com . Once RIM has reviewed your inventory form to ensure that it has been completed properly, RIM will forward your pick-up request to the storage vendor. This change in procedure is to ensure that the records are completely identifiable, easily retrievable and the information required for retention and destruction review is correct.

Complete the Inventory Form as follows:

Check whether it is Standard Storage or Climate Control Storage at the top of the form. Climate Control is used for electronic media. Do not mix electronic records with paper records. If you have both standard storage and climate control storage, you need to fill out a separate form for each type of storage.

ACCT. #: Fill in the storage vendor account number for your area. See the Storage Vendor Telephone Directory and Contact List for account numbers in your area.

PREPARED BY: Fill in your name.

PHONE NO.: Fill in your outside telephone number here.

DATE: Fill in the date the form is filled out.

DEPT: Fill in your department name or four-digit department number. Location number is not needed.

CARTON BARCODE: Place small die cut barcode label from the large barcode label sheet here.

RECORD CLASSIFICATION CODE: Fill in the Record Series # from MCI's Records Retention Schedule. RIM's website has a RS Code search function to help you identify code numbers; the link is below.

https://teamnet2.mcilink.com/departments/rim/retention/retention_form.html

DATE RANGE: Fill in From and Thru dates of records in carton. For example, if a box contains invoices from June 1996 to September 1996, you should fill in the "From" field with 06/01/1996 and the "Thru" field with 09/30/1996. If you only have a year, then span the entire year (i.e., 01/01/96 to 12/31/96).

RETENTION CODE: Leave blank, unless instructed otherwise by RIM. You would need to complete this field if you are storing active records, or records under litigation or audit; therefore, please call RIM for the code.

DESCRIPTION: 55 characters of descriptive information that FULLY explains the records in the carton. The description should be able to identify, to anyone within the company, the contents of the carton.

IMPORTANT:

The Inventory form is used to identify carton contents and ownership. It is also used to input carton information into MCI's national database of records. All storage vendors have been instructed, by RIM, to refuse pick-up of new storage cartons without accompanying inventory forms. In addition, all storage vendors have been instructed to return any cartons with an incomplete inventory form. Unique abbreviations, acronyms, numbers without qualifiers, individuals' names, terms such as: miscellaneous files, general files, desk files, old files, office files are unacceptable. Cartons containing these types of descriptions or cartons picked-up with no inventory forms will be returned to you. All costs associated with returning cartons to you will be charged to your department. If you have questions regarding acceptable/unacceptable descriptions, contact Phil Hasselvander at Vnet 806-3398 (703-886-3398) or Chris Moses at Vnet 806-7117 (703-886-7117).

Retrievals

Retrievals are those cartons that you wish to have recalled from the storage vendor and returned to you for temporary use. To retrieve cartons from storage, use the retrieval request

form on the RIM website. You will need to indicate which carton numbers you want retrieved from storage and delivered to you. You may only retrieve records stored by your department.

A department may not purge any records from a box that was retrieved from storage. Cartons that are retrieved must be returned to storage within 10 business days. For an exception to this policy, send an email to RIM at rim@mci.com with an explanation and justification for longer retention within the department.

Refiles

Refiles are those cartons previously retrieved from the storage vendor that you wish to have re-stored. To refile records with your storage vendor, use the pick-up request form on the RIM website to schedule carton pick-ups. To add cartons to your pick-up order, you must prepare a new request form.

Outcarded Records

All cartons retrieved from storage must be returned to the corrected storage vendor in 10 business days. If a department needs an extension, a written justification must be sent to RIM (rim@mci.com) from a Sr. Manager level or above with confirmation that all cartons are still in your possession and in tact. RIM receives a report, by contract, from each of the storage vendors identifying end-users who have withdrawn records past due. An email will be sent to those end-users who have had their records past due of the 10 limit to withdrawal. Sometimes an employee leaves the company while a box has been withdrawn in their name, in which case seek the alternate contact on the original retrieval request; if the alternate contact can't be found then the next manager up. In some cases a RIM staff member or someone from Facilities will have to be contacted, if no one is willing to claim the records, and a request to refile the said boxes would then be submitted.

Compliance Audits

All departments within MCI will be periodically audited by Records Management staff to:

- Ensure department compliance with record management policy and procedures.
- Is the department retaining their records for the correct period of time? The department needs to be accessed to ensure that they are not retaining their records too long nor too short a period of time.
- Is the department storing their records off-site properly? Can records be retrieved in a timely and efficient manner?
- Is the department destroying on-site records that have surpassed their retention?
- Is the department backing-up their PCs? Does the department maintain / retain e-mail properly?
- Review records retention period to comply with current financial, legal, operational/ revise as needed.

There are other criteria for passing the audit; however, the most important criteria is whether or not the department is retaining records they are responsible for, and retaining them for the right period of time.

Departments are selected for the audit at random (usually one out of each segment within MCI). The auditor performs background research on the department, such as finding out what types of records the department has, if they have off-site storage, etc. An e-mail, along with the audit questionnaire, is sent to the department requesting a meeting. During the meeting, the questionnaire is reviewed, along with follow-up questions. At the end of the meeting, the department is accessed for compliance.

Once the department has been audited, a memorandum is created stating the results and, any recommendations. The memorandum is sent to the Interviewee with a copy going to their manager. If the department passes the audit, a certificate is sent along with the memorandum. Departments that pass the audit are audited every five years. If a department fails the audit, the memorandum will contain reasons for noncompliance, recommendations to become compliant, and a re-audit date. Departments that fail are reviewed after three months to ensure they are moving forward with bringing their department into compliance, and then formally audited again nine months later.

E-Mail

The policy for electronic mail messages sent or received by company employees covers the creation and use of electronic messages, as well as access to and disclosure of these messages.

The policy includes all internal electronic mail systems, such as LANs, Outlook, Lotus Express, etc. The policy applies to full-time, part-time, and temporary employees, persons employed by temporary employment agencies, and to all third-party contractors with access to MCI MCI's electronic mail messaging systems.

All electronic communication systems and all communication and information transmitted by, received from, or stored in these systems are the property of the Company, and as such are to be used solely for job-related purposes.

Because e-mail encompasses the full array of types of communications, the retention period is based on the content of the message in question. Thus, for example, an e-mail message between a MCI employee and a vendor must be retained for the time period specified for vendor correspondence. Unless otherwise covered by a specific retention requirement, internal e-mail need not be retained beyond its useful life unless it is relevant to ongoing litigation, an enforcement proceeding or an audit. Under such circumstances, you typically will be notified of the obligation to retain until further notice the pertinent hard copy and electronically stored materials.

Imaging

If your department is interested in imaging their paper records, please call Records Management. We will work with you in determining your needs, whether your department needs to purchase the system, or if your documents can be placed on another imaging system within the company.

If you currently have an imaging system or are initiating one within your department, there may be IRS regulations or legal criteria that should be followed. A binder with the following data must be created and maintained on-site:

1. A record of where, when, and on what equipment any document was imaged will be maintained (to be retained in history format).
2. An accurate chronological record of changes to the system. This must be maintained for as long as the system is running.
3. Evidence of procedures ensuring quality, reliability and the integrity of the documents being imaged, including audit procedures.
4. A list of management personnel responsible for the supervision of the system (systems and record imaging). Provide names, dates, and titles. This needs to be updated when the "players" change.
5. Documentation on the initial system, and any significant change to the system. Any major changes need to be discussed with the Tax department.
6. A description of the optical platters used for storage, and location of where back-up copies will be maintained.
7. Identify the location of records that are not or cannot be imaged.
8. Procedures for retrieving records from imaging system.

Originals of imaged documents need to be retained if the retention period is longer than 7 years. Imaging systems should be used for day-to-day use and the need for quick retrieval, not for long-term storage.

If implementing an imaging system for financial records, IRS Rev. Proc. 97-22 and 98-25 must be followed. Records Management has a copy of both revenue procedures, as does the tax department.

Back-up copies of imaging platters or electronic media (CD ROM, tape, diskette, etc.) must be retained away from the location of where they are being created or used. RIM recommends that the back-ups be placed in off-site storage within a climate-controlled vault. Much like tape storage, there should be a *floor copy* that is used as the working copy, and a copy used for disaster recovery. If anything happens to the *floor copy*, the disaster recovery copy is pulled from storage, copied, and returned to storage.

RIM is your source for any questions or directions pertaining to the maintenance, retention, storage and destruction of all MCI records.

Please contact RIM….we are here to assist you.

Following is the Memo, approved by Michael Cipichio, is accompanying the Questionnaire that follows.

In an effort to promote awareness of and conformance with MCI's Record Compliance Program and policies, Records and Information Management (RIM) requires your support. RIM has produced a questionnaire, which can be accessed at https://teamnet2.mcilink.com/departments/rim/inform/questionnaire.html Its purpose is to assess your organization's functions, its records, and its record retention practices. We ask that you assist RIM to ensure that your organization is aware of and adheres to our Record Compliance Program. Please return the completed questionnaire to James Green. By _____ *Each Department must complete a Questionnaire*.

Proper retention of records is critical from a financial, legal and operational standpoint. Accordingly, as a MCI employee, you are responsible for understanding the policy and complying with the program. The Company must adhere to all local, state, federal and operational record keeping requirements, therefore, compliance is mandatory. The program also offers many practical advantages, including opportunities for off-site storage that can save valuable office and computer server space while improving office workflow.

Information concerning MCI's document retention policy and program is located at https://teamnet2.mcilink.com/departments/rim. This website contains valuable information including, but not limited to:

1. Company policies and procedures on records management.
2. A searchable retention schedule
3. Guidance on what records are considered confidential

Your support is appreciated. If you have any questions or comments about the program or the questionnaire, please contact any of our RIM personal. The directory for all RIM staff is located at https://teamnet2.mcilink.com/departments/rim/phone/contacts.html.

RECORDS MANAGEMENT QUESTIONNAIRE

A separate questionnaire must be completed by each department.

After RIM has reviewed the completed questionnaire, you will be contacted by telephone with follow-up questions and pertinent records guidance where necessary.

Date:	
Company Name:	
Name:	Title:
Phone Number:	Email address:
Department Name (and number)/Division:	Address:
Senior Manager's Name:	Email address:
Director's Name:	Email address:

At various points in this questionnaire you may be requested to provide a copy of additional materials; please use the following address:

MCI
Attn: James Green
22001 Loudoun Country Parkway
D1-3-375
Ashburn, VA 20147

Or email: james.green@mci.com

1. What category does your department fall under?
   Pick one:

Accounting	**Marketing**
Administration	Sales
Corporate	Network Services
Finance	Systems
Human Resources	Tax
Legal	

2. What is your department's primary function?

3. What types of records/information is your department responsible for?

4. From *whom/where* does your department receive records/information (e.g., department name, outside company/agency name, etc.)?

5. In *what form* are the records/information received?
   Pick all that apply:

Paper	Mainframe
Microfiche	Mid-Range
Microfilm	Diskette
Tape	Electronic
EDI	CD
Optical	

6. To whom does your department send records/information (e.g., department name, outside company/agency name, etc.)?

7. In what form is the records/information sent?
   Pick all that apply:

Paper	Mainframe
Microfiche	Mid-Range
Microfilm	Diskette
Tape	Electronic
EDI	CD
Optical	

8. In what form do your records/information reside?
   Pick all that apply:

Paper	Mainframe
Microfiche	Mid-Range
Microfilm	Diskette
Tape	Electronic
EDI	CD
Optical	

9. Has the department ever inventoried all of its records?
   a. Yes
   b. No

If yes, please provide a copy of the inventory.

10. Do you have records/information stored off-site?
    a. Yes
    b. No

11. If yes, do you have a contract with an off-site storage vendor?
    a. Yes
    b. No

If yes, please provide a copy of the contract and the company contact.

12. Does your department use the LAN to store records/information?
    a. Yes
    b. No

13. Does your department use the LAN to share records/information with other groups?
    a. Yes
    b. No

14. Does the department purge records/information from the LAN?
    a. Yes
    b. No

15. Does the department use or own any other servers (i.e., web, mid-range, etc.)?
    a. Yes.
    b. No

If yes, what?

16. Does the department back-up its computers?
    a. Yes
    b. No

17. Does the department have laptops, desktops or both?
    a. Laptops
    b. Desktops
    c. Both

18. Are employees required to take the laptops home or secure them in the office?
    a. Take Home
    b. Lock Up
    c. Either
    d. Neither required

19. What percentage of on-site records are inactive (used less than once a month)?

20. Are your records originals or copies?
    a. Originals
    b. Copies
    c. Both

21. What percentage are originals?

22. Does the department generate the originals or are they sent to you by others?
    a. Generate originals
    b. Sent by others
    c. Both

23. Does the department generate the copies it maintains or are they sent to you by others?
    a. Generate copies
    b. Sent by other departments
    c. Both

24. Do you have a central filing area or file cabinets throughout the department?
    a. Central filing area
    b. Cabinets throughout
    c. Neither
    d. Both

25. Are files retained in employee's offices or cubes?
    a. Yes
    b. No

26. Is your floor or area accessible by anyone during work hours?
    a. Yes
    b. No

27. Do you know where your system back-ups are being stored?
    a. Yes
    b. No

If yes, where?

28. Who, within your department, is responsible for retaining records on-site and/or storing records off-site? Please provide name(s) and telephone number(s).

APPENDIX L

Compliance Audit Exhibits

APPENDIX M

RRI

List of HLQs and Required Retention

APPENDIX N

LPP's

"E-Mail Guidelines"

-----Original Message-----
From: **O'Neil, Thomas F.**
Sent: Sunday, October 31, 1999 10:12 PM
Subject: E-Mail Guidelines

Attached are E-Mail Guidelines which we have drafted to address various legal risks created by the Company's extensive use of e-mail as a preferred mode of communication. The Guidelines include various practical suggestions about drafting and retaining e-mail messages. I would very much appreciate your forwarding electronic or hard copies of this document to all appropriate personnel in your respective organizations. Feel free to call me if questions arise as folks review it.

Thanks very much.
Tom O'Neil
Chief Litigation Counsel

E-Mail Guidelines[1]

Thomas F. O'Neil III

Chief Litigation Counsel
MCI, Inc.

Based in large part on lessons learned from extensive internal review of records in connection with civil litigation and enforcement proceedings, we have drafted the following Guidelines concerning the use, content and retention of electronic mail ("e-mail"). Virtually all MCI, Inc. ("MCI" or the "Company") employees now rely heavily on e-mail as the primary mode of business-related communication and, for the reasons set forth below, it is critical that you use it carefully.

Many people treat e-mail exchanges casually--indeed cavalierly--as if they are equivalent to a private telephone conversation. This approach can subsequently jeopardize the Company's interests in a way that typically is never envisioned when the message is drafted. That is because unlike a telephone conversation that ends when the call is terminated, an e-mail message is a written communication that creates a record, which can easily be forwarded, printed, and stored electronically, and which often cannot be truly deleted or discarded by the author or the recipient. Like other written materials, individuals, entities and regulatory officials can obtain our e-mail through discovery mechanisms in civil and enforcement proceedings. Accordingly, whenever you address a sensitive subject, such as technological or fiscal feasibility, or the ethical or legal permissibility of a new product, service or strategic proposal, you should consider using alternate means of communication, such as a meeting or a conference call. We hope these Guidelines will assist you in making that assessment.

I. THE CONTENT OF E-MAIL MESSAGES

A. Overview

1. Internal Messages

Although internal e-mail messages, by their very nature, tend to be less formal than external correspondence, you always should compose and transmit them with the understanding that they may well become public. If an e-mail would tend to confuse or embarrass you or the Company in a public forum, such as a deposition, a legislative hearing or a judicial proceeding, it should not be issued. This litmus test applies with equal force to the full gamut of messages, from highly personal musings to potentially troublesome reflections or admissions concerning pending business transactions. For this same reason, in drafting any e-mail message, you should not engage in unnecessary speculation about, for example, the motive's of a particular person or the outcome of a pending transaction.

Unintended disclosure of an internal e-mail message can occur in several ways. It might, for example, erroneously be sent to an inappropriate recipient as a result of the use of a wrong key – *e.g.*, the "Reply All" function. At the same time, a recipient of an internal e-mail may forward it to an external party, naively trusting that recipient not to store or further transmit it. Finally, as previously noted, e-mail messages, unless covered by a recognized privilege, are subject to discovery in litigation, congressional investigations and regulatory enforcement proceedings.

2. External E-Mail Messages

As we all know, e-mail has virtually replaced hard-copy correspondence. Although e-mail messages are easier to compose and send than traditional letters, legally there is no distinction between them. Therefore, as with any written corporate communication, an external e-mail should express well-formulated and well-articulated thoughts. "Thinking out loud" is particularly inappropriate for such a message. In short, you should draft an external e-mail message with the same level of care and formality with which you would draft a business letter to the same recipient.

B. Recommendations

With these content-based cautions in mind, we offer the following guidance. If a gratuitous comment could subsequently embarrass you, – for example, "Customer 'X' is sleazy;" "The regulators are crazy," or "Let's call Legal and say that we never understood the contract when we signed it," do not type it. In the same vein, if you receive a message that evokes an emotional response on your part, be wary of answering by e-mail. At a minimum, wait until you are able to review it objectively for tone and content, and then reconsider the propriety of responding by way of e-mail.

We are all best-advised not to discuss via e-mail the question whether the Company, one of its subsidiaries, or one or more of its officers, directors, or employees has acted properly in certain circumstances. Never discuss or debate the legality of a situation through e-mail. It is equally unacceptable to suggest in e-

mail that legal advice be ignored. Finally, detailed discussions of sensitive strategic questions should never be pursued electronically.

II. PROPRIETARY OR PRIVILEGED INFORMATION

A. Confidential/Proprietary E-mails

Given the Company's preeminent position in a frenetic industry, it is inevitable that at some point you will need to resort to e-mail to transmit internally confidential or proprietary information, such as strategic planning documents, confidential customer information, and proprietary technical information. But before disseminating that type of information, you should consider the attendant "cyber-risks." If you decide to proceed, the message should include the following header: "CONFIDENTIAL INFORMATION – PLEASE DO NOT FORWARD, PRINT OR STORE ELECTRONICALLY." Because claims of confidentiality can be rendered vulnerable by overuse or misuse, this header should be used consistently and only when the e-mail actually contains confidential or proprietary information. When in doubt, please use the header.

B. Legal Privileges and E-mail

Some e-mail messages may be covered by legal "privileges" that may protect them from disclosure. The most common of these is the attorney-client privilege.[2] Essentially, it applies to a confidential communication between a lawyer and a client (or the agent of either) for the purpose of obtaining legal advice. More specifically, in the corporate setting, the attorney-client privilege applies where (1) counsel is acting in a legal capacity, (2) the communication was understood to be confidential when made, and (3) the communication is disclosed only to essential corporate employees. The following maxims apply to privileged communications:

1. Use e-mail to disseminate privileged communications only when necessary. As noted, you should always try to avoid discussing via e-mail legal strategy, or to exchange privileged drafts of letters, contracts or pleadings. To the extent possible, messages seeking legal advice should not include unnecessary business discussions.

[2] For a detailed discussion of the attorney-client privilege, visit the LPP website at https://teamnet2.mcilink.com/departments/lppgc/

2. Merely "cc-ing" a lawyer on an e-mail message will not transform it into a privileged communication. It must satisfy the criteria of the test set forth above. To determine whether a communication truly is for the purpose of obtaining legal advice, a court will consider whether it is addressed directly, and primarily, to counsel and, even more importantly, whether the text of the message supports the claim of privilege.

3. Every privileged communication should be clearly marked "PRIVILEGED AND CONFIDENTIAL; SUBJECT TO THE ATTORNEY-CLIENT PRIVILEGE." As with e-mail messages reflecting confidential or proprietary information, this header should be used consistently and after careful consideration of its applicability. Generally, you should use it whenever you send an e-mail message to an in-house lawyer seeking any sort of guidance.

4. Insofar as confidentiality is concerned, you should not disclose the contents of a privileged communication to anyone other than an employee of the Company who has a very real "need to know." As noted above, copying or forwarding a privileged e-mail message to anyone else most likely will waive the privilege.

5. When possible, maintain all privileged communications in separate, clearly labeled files.

III. DISTRIBUTION AND PRESERVATION OF E-MAIL MESSAGES

A. Broadcast E-Mails

E-mail enables an author to distribute a message to a broad audience in a matter of seconds. Although it may be critical in certain situations, such broad distribution of e-mail should not be the routine approach. Indeed, the Company has issued a Broadcast Messaging Policy requiring all such transmissions to be channeled through Corporate Employee Communications and subject to the approval of senior management.[3]

B. Forwarding E-Mail Messages

As a general rule, you should exercise great caution when forwarding comprehensive e-mail messages. In short, do so only when absolutely necessary. "Chain" or "nested" e-mail messages--i.e., those attaching a string of prior messages--present special concerns. Forwarding an otherwise privileged message to a non-lawyer or someone not employed by the Company typically will cause the protection afforded by the privilege to evaporate. Alternative approaches to consider here are drafting an entirely new message summarizing the key points, or "cutting and pasting" pieces of messages into a new, more succinct one.

[3] The Broadcast Messaging Policy can be found at https://teamnet2.mcilink.com/departments/public_relations/messaging_policy/index.html.

C. Retention of E-Mail Messages

The Company has in place a mandatory records retention policy developed and monitored by our Records Management Department. This policy applies to all MCI entities and establishes retention criteria, which are generally based on the nature or content of a particular document. Because e-mail encompasses the full array of types of communications, the retention period is based on the content of the message in question. Thus, for example, an e-mail message between an MCI employee and a vendor must be retained for the time period specified for vendor correspondence.[4]

Unless otherwise covered by a specific retention requirement, internal e-mail need not be retained beyond its useful life unless it is relevant to ongoing litigation, an enforcement proceeding or an audit. Under such circumstances, you typically will be notified of the obligation to retain until further notice the pertinent hard copy and electronically stored materials.

* * *

These Guidelines do not address every question that will arise in connection with e-mail usage. You should feel free, therefore, to call me (v222-6412/202-736-6412), Adam Charnes (v222-6093/202-736-6093) or Jamon Jarvis (v222-6342/202-736-6342) if you need more focused advice.

[4] For additional information regarding record retention policies, please consult the Records Management Department.

APPENDIX O

Training Presentations

Records and Information Management

RECORDS COMPLIANCE PROGRAM

RIM's Website:
https://teamnet2.mcilink.com/departments/rim/

MANDATORY PROGRAM

- The Company and its employees must adhere to all state, federal and operational record keeping requirements.
- All levels of management are held accountable for their department's compliance.
- Adherence to the Program and the requirements outlined in the Record Retention Schedule is mandatory, without exception.
- Each department will be audited periodically for compliance.

Records & Information Management

SCOPE AND OBJECTIVES

- Identify and Secure Vital Records.
- Institute a Disaster Recovery Plan for all company records and information.
- Ensure legal compliance and audit protection.
- Minimize litigation risks.
- Assimilate new records management technologies.
- Access to valuable information and costs saving.

A RECORD IS…

A record is any or all recorded information, regardless of medium or specific characteristics, created, received, used or distributed by MCI in the course of its business. This includes paper, microfilm, tape, microfiche, e-mail, PC hard drives, mainframes, mid-range systems, voice mail, optical, intranet and other mediums.

Only the *official copyholder* of a record is required to retain a record for the total retention period indicated in the RRS. If you maintain originals, you are the official copyholder. Creating a record does not mean you are the official copyholder; you must also maintain the original. Copies should not be stored or kept once your operational need is completed.

Drafts documents should not be retained once a document is finalized. Drafts have no retention requirement and must not be retained in any media form. However, it is acceptable to hold drafts until a document is finalized, then they should be purged.

E-MAIL

E-mail is just another form in which records/information is received.

- E-mail received or created in the course of business is an official record. It is the message within the e-mail that should be considered for retention, not who the message is from.
- The retention period is based on the content of the message. For example, an e-mail message between a MCI employee and a vendor must be retained for the time period specified for vendor correspondence.
- Keep in mind that, approximately, one percent or less of all e-mail sent or received has a true retention value. For internal e-mail messages, the sender has the obligation to follow any retention requirements, not the recipients. For e-mail messages coming from an external source, the recipient needs to either purge or retain pursuant to the Records Retention Schedule. Since a majority of e-mail has no retention requirement, all employees should be deleting e-mail once the retention requirement or operational need is complete. Operational need should not exceed one year from the receipt or sending the message.
- Specific company policy on e-mail, as written by Legal, can be located at: https://teamnet2.mcilink.com/departments/lppgc/techlaw/

VITAL RECORDS

- Vital records contain information that is essential to reestablishing or continuing an organization in the event of a disaster.
- Vital records are essential:
  - to continue Company operations,
  - to recreate the Company's legal and financial position, and
  - to preserve the rights of the Company, its employees, customers, and stockholders.
- Examples of Vital Records are: ledgers & journals, customer billings, mergers, articles of incorporation, patents/copyrights and stockholders registers, design/documentation.

DISASTER RECOVERY PLAN

Used in the salvaging of records of various media types (paper, CDs, diskette, tape, electronic, etc.) when disaster strikes.

- Focus of the plan is designed to:
  - minimize disruption of normal business operations
  - prevent further escalation of the disruption
  - minimize the economic impact of the disaster
  - establish alternative operating procedures
  - recover/salvage organizational assets
  - provide for rapid and smooth
  - train personnel with emergency procedures
- Each department responsible for Vital Records must have a Disaster Recovery Plan.
- The Plan must be provided to Records and Information Management.

WANT TO IMAGE YOUR RECORDS? ALREADY DOING SO?

- Is imaging a cost effective way to handle your records versus using off-site storage? If using off-site storage, you can have your records within 2 hours.
- Imaging systems should be used for day-to-day use and the need of quick retrieval, not for long-term storage.
- Originals of imaged documents need to be retained if the retention period is longer than 5 years; however, you must get written approval from RIM, Legal and Tax to destroy the originals after they have been imaged.
- If initiating an imaging system with your department, there may be IRS regulations or legal criteria that should be followed. RIM or the Tax department can provide a copy of the revenue procedures.
- A binder with the following data must be created and maintained on-site:

1. A record of what you are imaging, where, when, and on what equipment any document was imaged will be maintained (to be retained in history format).
2. An accurate chronological record of changes to the system. This must be maintained for as long as the system is running.
3. Evidence of procedures ensuring quality, reliability and the integrity of the documents being imaged, including audit procedures.
4. A list of MCI management personnel responsible for the supervision of the system (systems and record imaging). Provide names, dates, and titles. This needs to be updated when the "players" change.
5. Documentation on the initial system, and any significant change to the system. Any major changes need to be discussed with the Tax department.
6. A description of the optical platters used for storage, and location of where back-up copies will be maintained.
7. Identify the location of records that are not or cannot be imaged.
8. Procedures for retrieving records from imaging system.

MANAGER RESPONSIBILITIES

- All Managers' working files for employees should be sent to the HR Fileroom once an employee no longer works for the company or your department. If an employee transfers to another department, you should send any manager notes regarding the employee to the HR Fileroom. It is acceptable, however, to give the new manager the employee's attendance record, performance review and PAF, but you cannot give those notes or written comments that are about or concern the employee.

- The HR Fileroom is located at: 9835/700, 707 17th Street, Denver, Colorado 80202

- When an employee leaves the company, all files on his/her computer must be reviewed (including e-mail and e-mail attachments) for retention requirements under the Records Retention Schedule. The computer's records should be either retained or destroyed. Files that require retention must be pulled off the computer and stored appropriately. After this review, the computer's hard drive must be wiped clean of all records before being issued to a new user (even if this new user is in the same department).

- If a Manager receives a request from a terminated employee regarding getting copies of their travel and expense records or records contained within their personnel file, the Manager must refer the terminated employee to Law & Public Policy (LPP). No records or information may be given out to terminated employees (voluntary or involuntary) without prior approval from LPP.

RECORDS RETENTION SCHEDULE (RRS)

Record Retention

- A tool that identifies those records requiring retention and their required retention period.
- The retention periods in the RRS are based on federal, state or local regulations and the company's operational needs.
- Retaining records longer than their legal or operational requirement exposes MCI to unnecessary financial and legal risk.
- MCI must avoid the perception that we are selectively disposing of records.
- Primary objective is for prompt disposal of records whose retention period has been met.
- Based on the company's functional areas and records common to those areas.
- Assigns each "type" of record its unique Record Series (RS) number. Determination, by the user, of the correct RS number is important in calculating the correct destruction review date.
- "Just in case" is not a consideration in retention. Individual departmental determinations do not supersede or replace the MCI Record Retention Schedule. Requested exceptions are submitted to RIM.

RECORDS MANAGEMENT COMPLIANCE AUDIT

Some factors for compliance:

- Are all employees aware of and in compliance with the retention program?
- Does the department recognize what a record is?
- Is the department reviewing and retaining their records, on-site & off-site, in accordance with the Record Retention Schedule?
- Is your department storing their records off-site properly?
- Can records be retrieved in a timely and efficient manner (off-site and on-site)?
- Does your department recognize that e-mail and anything downloaded from the internet are records?
- Is your department deleting e-mail and electronic data when operational need or legal retention requirements are surpassed?
- Does your department handle Vital Records?
- Does your department have a Disaster Recovery Plan?

If you want to make sure that you department is compliant with the Records Management Program before a formal audit is conducted, please call RIM.

OFF-SITE STORAGE

Off-Site

- All procedures associated with off-site storage are detailed on RIM's website.
- What you put into storage is your individual responsibility. If someone tells you to send something to storage (or retain it on-site) and you know it is against retention policy, you must challenge that request.
- All costs are paid by the RIM department, with the exception of:
  - Cartons returned to the submitter because of absence of inventory data.
  - Non-response to service request. You requested service from the storage vendor, but both you and your designated alternate point of contact were not present when the vendor's 'driver' arrived to deliver/pickup.
  - Rush orders.
- Any questions or problems that you have about off-site storage, contact RIM. Do not contact the storage vendor.
- Review the records you are planning to archive to ensure they have a retention requirement. Only those records should be placed in off-site storage.
  - No copies, working papers, drafts, miscellaneous manuals, stuff from past employee's office/desk (w/o review), no data in electronic form unless the associated software/hardware system is retained.
- Standard Storage & Climate-Control Storage.
  - Climate controlled storage is available for records retained on such media as microfiche, CD, tape, etc. You must indicate this type of storage to the vendor (on the MCI Inventory Form) when submitting the materials to storage.
- Only 'like' records can be put in to each storage carton.
  - Invoices separated from correspondence. They have different RS codes – have different retention requirements.